INVITED PAPER

High-Assurance Smart Grid: A Three-Part Model for Smart Grid Control Systems

Cybersecurity and control for future Smart Grid systems is the topic of this paper, which recommends distributed control for grid management and hierarchical control for planning and dispatch.

By Thomas M. Overman, *Member IEEE*, Ronald W. Sackman, *Member IEEE*, Terry L. Davis, *Member IEEE*, and Brad S. Cohen

ABSTRACT | As electrical grids evolve through the introduction of additional "smart" sensors, actuators, and control systems, cybersecurity becomes an ever more significant factor, necessitating the incorporation of Information Assurance principles throughout the electrical system—from central station power generating facilities, through transmission and distribution systems, to building management systems, distributed generation, home area networks, and plug-in hybrid electric vehicles. A precursor to determining the appropriate controls for any particular device within this complex system is to determine the trust model (or untrusted condition) within which the device exists. This paper, then, sets out to define a multilevel framework for an architecture to be used throughout the electrical system—a High-Assurance Smart Grid architecture that incorporates three core attributes:

1) categorizes cybersecurity requirements based on a multi-tier determination of a subsystem's potential impact on the overall system;
2) implements a robust defense-in-depth cybersecurity architecture;
3) implements a distributed rather than hierarchical control system architecture based on an assumed compromise (untrusted condition) of system control components and subsystems using autoresponsive (AR) load control wherever possible.

Manuscript received April 28, 2010; revised September 30, 2010 and December 21, 2010; accepted January 18, 2011. Date of current version May 17, 2011. This work was supported by The Boeing Company.

T. M. Overman and **R. W. Sackman** are with The Boeing Company, Sunnyvale, CA 94085 USA (e-mail: toverman@ieee.org; ronald.w.sackman@boeing.com).
T. L. Davis was with The Boeing Company, Everett, WA 98204 USA. He is now with iJet Onboard, Seattle, WA 98101 USA (e-mail: tdavis@ieee.org).
B. S. Cohen is with The Boeing Company, Hazelwood, MO 63042 USA (e-mail: brad.s.cohen@boeing.com).

Digital Object Identifier: 10.1109/JPROC.2011.2112310

Multitier approach. It has been recognized by the Federal Energy Regulatory Commission and by the National Institute of Standards and Technology that a criticality model that simply defines grid controls as either critical or noncritical is insufficient. We therefore look to an analogous multitier system impact model from aviation that may provide a useful model for the power grid.

Defense-in-depth. Best Practices in Information Technology use a set of protective systems in order to form a defense-in-depth approach to shield critical systems. The defense-in-depth principle is more than a ploy to "keep out" threats; rather it assumes the threat *may already exist within the environment*, whether through malicious intent or the mistaken actions of untrained or distracted personnel. As the electrical system is transformed through the introduction of significant numbers of intelligent electronic devices, the value of incorporating more cybersecurity controls from the IT domain is recognized as being of increasing importance.

Assume compromise of control systems and implement AR load control where possible. Rather than attempting to create an all encompassing enclave of trust, the control system architectural model proposed here suggests systems should be designed with the expectation that adjacent systems *will be* compromised, understanding that an expansive sphere of implied trust inevitably leads to an expansive sphere of vulnerability. Holding an expectation of compromise—a lack of trust (untrusted condition)—is the preferable stance, because it in turn requires that subsystems implement independent rather than dependent cybersecurity and energy control data flows and allows evolving threats to be countered without continual system updates.

Once an assumption is made that every command and control (C2) system has a variety of failure modes, consideration

should be given to determining where the use of explicit C2 can be avoided while still achieving some of the goals the C2 system is intended to provide. Many demand-response (DR) functions exist to enable operating utilities to reduce loads in anticipation of or in response to grid overload conditions. AR load control can provide the desired DR without the need to build hierarchical C2 capabilities all the way back to the control room. Thus the distributed nature of the recommended architectural approach incorporates both distributed-but-collaborative decision making and autonomous decision making.

KEYWORDS | Centralized control; control systems; distributed control; industrial control; information security; intelligent control; power grid; power systems control; Smart grid

I. INTRODUCTION

The electric system encompasses everything from power generation to transmission and distribution systems, and the electrical loads connected to the system. It also includes both centralized and distributed power generation and storage systems that vary in scale by several orders of magnitude. This system can be viewed as a networked system of systems, or a networked grid of grids, with literally millions of nodes. There have already been numerous cases of control system cyberincidents in the North American Electric System [1]. As the implementation of additional programmable electronic sensors and actuators becomes more pervasive over the coming decades, implementing appropriate cybersecurity controls will become even more critical to the overall health of the system.

In such an extensive and diverse grid of grids, it is neither possible nor necessary to establish peer trust relationships between every device in the system (e.g., a home water heater and a transmission substation actuator have very different impacts on the overall grid).

Over the past two decades, the aviation industry has been addressing the security of integrated sensors and actuators made by several vendors and integrated into a single system. The model proposed here is based to some extent on the model used in the aviation industry for categorizing various control subsystems by their criticality to the overall system (the airplane) [2], [3]. The model defines three categories based on the impact of a subsystem failure (catastrophic, major, and minor impact) to the grid. The initial guidance shown in [2] gives three levels of subsystem impact. In this case, discussion of how these levels may apply to the grid is given as follows:

1) Level A (or High): failure of these systems are likely to cause failure across tens of thousands of nodes;
2) Level B (or Medium): failure of these systems may cause loss of power to hundreds or even thousands of nodes in a smaller geographic area;
3) Level C (or Low): failure of these systems may cause localized failure.

The aviation model also defines Levels D and E, which have even lower impact. These may be applicable for uses like home metering, some industrial metering, and some system metering needs.

The second principle to be taken from aviation [2] is the concept of fail-safe operation. Avionics systems must be designed in ways which *expect* failure of adjacent systems. From a Smart Grid Cybersecurity perspective, rather than attempting to create an all encompassing enclave of trust, this model suggests that systems should be designed in ways which *expect* compromise of adjacent systems (whether through system failure, user error, or malicious activity).

Certainly, a number of steps must be taken which, together, provide a defense-in-depth architecture for grid control systems. IT best practices combine several cybersecurity systems such as firewalls, role-based access control (RBAC) functionality, malicious software protection systems, encryption of data at rest and in transit, and host and network intrusion detection systems, to name just a few such systems. All of these and more are necessary parts of a modern control system architecture.

Significant discussion has been offered by numerous authors over the past few years about cybersecurity threats to grid control systems. These authors firmly believe that many of the threats they address—from nation-state actors, to cyberterrorists, to sophisticated criminal organizations—are very real and tangible. Thus, employing defense-in-depth methodologies, including fail-safe devices and fail-secure functionality, is a necessary part of any serious effort to protect grid control systems.

However, even a robust combination of such security systems is not sufficient for today's, much less for tomorrow's, increasingly complex control systems. This is especially true when operations must continue despite failures while ensuring reliability of the electric grid that is equal to or better than what is possible today. In reality, the accumulation of hundreds, thousands, and potentially millions of additional grid sensors and actuators will have the advantage of providing grid operators with substantially improved fidelity of status and control over electrical grids. However, these modern sensors and actuators are more complex than their electromechanical predecessors. This increased complexity, at both the individual device level and the overall system level, at the same time introduces more inherent fragility than exists with the traditional electromechanical controls. Whereas there are many examples of fully functional grid actuators that have been in service 40 or more years, many electronic control system components have not even existed for one-twentieth of that service life. Consequently, there is no real service life history (as opposed to test-based projections) to demonstrate that the new technologies will have the same reliable service life as traditional systems.

The fragility of the new grid devices and the possibility of cyberattack or inadvertent action of potentially untrained or distracted employees increase the likelihood of unplanned outages to the control system components themselves. When this is added to the well known grid vulnerabilities from unplanned line outages, higher than expected loads, and loss of generation capacity, reliability challenges are further increased. The widespread introduction of intermittent generation sources will further exacerbate this situation. Rather than creating an unsolvable problem, however, this combination of traditional and new vulnerabilities provides an opportunity to rethink the underlying architecture of the grid control systems themselves.

Before delving into further detail, it is worth addressing at least two distinct definitions of "High Assurance." One definition of High Assurance System Engineering characterizes systems as being reliable, available, safe, secure, and timely [4]. Another definition is related to formal Evaluation Assurance Levels, EAL-6 and EAL-7 [5], [6]. In our view, rather than being competing definitions, the EAL approach can be viewed as a subset of the broader field of High Assurance System Engineering [7].

II. AVIATION RELIABILITY CONCEPTS

A commercial aircraft is arguably one of the most complex systems ever devised. Planes can only take off and land at a relatively small number of places on the globe, and then in only a very precise manner to achieve safe departures and arrivals, yet commercial aviation remains by far the safest and most reliable way to travel. How the aviation industry accomplished this remarkable engineering feat of safety and reliability while at the same time making a commercial aircraft that requires relatively light daily/weekly maintenance and utilizes straightforward routine maintenance processes may yield design concept parallels applicable to the electrical grid. While both aviation and electrical grid subsystems historically were specialized, purpose-built devices, in both of these industries there is a significant transition toward more general purpose computing platforms. Thus both industries face similar challenges in that the relative obscurity and lack of connectedness which protected many systems is rapidly diminishing.

At the core of aircraft design is the concept that an aircraft is not a single huge complex system; rather it is *a large set of relatively small semi-independent systems*, each of which mostly performs a small set of similar or related tasks. Within an aircraft, each system is categorized by criticality as mentioned above. Systems have small, straightforward, tightly specified interfaces with only a small number of other aircraft systems of the same criticality on which they either rely for information or which rely on them for information.

Each system design must take into account how the failure of systems with which it communicates or interfaces would be impacted by its failure. Design contingencies must be incorporated so subsystems respond appropriately to the loss of an interfacing system, and a certification process must demonstrate how the impact of failures in adjacent systems has been mitigated to the level required for its individual reliability requirements. It is important to note that a "Level A" flight-critical system cannot rely on a lower criticality system for security or functionality, as the lower level systems do not have the same design reliability requirements. For critical systems, enhanced designs to meet the required reliability often require redundant systems and even inter-system voting algorithms [8].

The Bulk Electrical System has a requirement to have what is called N-1 reliability [9]. In this concept, no single failure can have a catastrophic impact on the overall electrical grid. Aviation reliability requirements, in contrast, have what may be called N-3 reliability. This is discussed in Appendix H of the FAA System Safety Handbook, which is also published as MIL-STD-822D [10]. Reference [10, Sec. A.4.3.3.1.2.b] states the requirement: "For safety critical command and control functions: a system design that requires at least three independent failures, or three independent human errors, or a combination of three independent failures and human errors."

This design philosophy yields an overall system where cascading system failures can be controlled and minimized. The fault trees for an event can be readily developed and understood for a given system, as it has a limited number of well-defined inputs and a limited set of systems it relies upon. Besides establishing a high level of reliability, this ability to have well-defined fault trees also assists the process of defining the corresponding fault isolation and maintenance actions in a relatively straightforward manner.

Add to this the fact that the base operating code to support a single system is stripped down to an absolutely minimal size containing only code that is required by that system's functions; thus reliability and fault isolation are again enhanced. Minimizing the code size of the module then allows for the module to be inspected and tested more simply. The constraints on inter-system dependencies, limited message and sensor inputs, and minimal code additionally allows for reasonable set up of high-integrity tests to be run against it to validate its reliability.

Another key concept of aviation system design is that its interfaces are "*message-based*" *rather than the typical Internet reliance on the more open* "*connection-based*" *application communication designs*. The reliance on "message-based" interfaces allows the system code to protect itself against basic message errors—however they occur. Un-requested responses, oversize responses, data fields that do not match the data label in type or size, corrupted messages, out-of-bound inputs, etc. can all be

handled by the system design, allowing it to be designed and tested to meet its specific reliability requirements.

Aviation Cybersecurity. As a side benefit of the overall avionics design philosophy, systems designed in this way present a minimal surface for cyberattacks. A system has only a small number of other systems it relies upon and communicates with, and it carries only the operating code necessary for its own functionality. And these systems have a detailed interface specification that includes the expected data/sensor exchanges, a detailed data label, and the expected data interchange rates and latencies. These attributes taken together both enhance the effectiveness of classic cybersecurity technologies and allow unique engineering of the system to deal with interfacing systems that are misbehaving or fail for whatever reason.

Finally, in the area of aircraft-to-ground communications, aviation utilizes a single global communications network that is defined at the International level by the International Civil Aviation Organization (ICAO) [11]. This common infrastructure extends to "common defined messages" for all digital communications to or from the aircraft, extending the onboard "message based" interface standards to include the supporting ground infrastructures. Since these communications systems are based on the Open Systems Interconnection (OSI) Reference Model and predate current cybersecurity technology, today all flight-critical digital messages are pilot-mediated. However, aviation is planning on the Next Generation of Air Traffic Management (ATM) networks, as well as current aviation business-to-business (B2B) networks, to be based the Internet Protocol (IP) and Internet related protocols (i.e., the IP Suite). To that end, aviation is working toward standardization that will facilitate global use of IP and its associated security protocols for both ATM and B2B. This is similar to control systems in the electric system.

Initial work identified Public Key Infrastructure (PKI) certificate compatibility as a key issue for B2B utilization. To ensure that compatibility, the aviation industry has created both a PKI reference model and the Air Transport Association "Specification 42" [12] to define PKI infrastructure and certificate use. In addition, via the aviation standards organizations and the Internet Engineering Task Force (IETF), aviation has initiated discussions with the communications and systems vendors to develop global standards for testing and certification of the interoperability of the key security protocols, "Internet Protocol Security (IPsec)" and "Internet Key Exchange-Version 2 (IKEv2)," to ensure their viability for aviation uses globally to create a "defense-in-depth" aviation cybersecurity architecture extending from core aircraft system designs through the communication layers. Recent efforts by the National Institute of Standards and Technology (NIST) in forming the Smart Grid Interoperability Panel (SGIP) [13] are an obvious parallel with ongoing activities within the aviation industry.

Fig. 1. ***Legend for impact of failure.***

III. IMPACT OF FAILURE IN THE ELECTRICAL GRID

Using the multi-tier model for criticality discussed above, it is relatively straightforward to construct a macroview of how this can be applied to the electrical grid over a large area. In this view, we define three impact levels: High, Medium, and Low. Fig. 1 provides a color key to the designated impact levels in subsequent illustrations. In their 2009 Concept Paper *Categorizing Cyber Systems: An Approach Based on BES Reliability Functions* [14], the North American Electric Reliability Corporation (NERC) recommends a similar approach. The same relative analysis is possible with more criticality levels (as in aviation), but having fewer than three criticality levels seems unlikely to provide sufficient differentiation.

Using the three-level model, the following is a typical analysis of the power grid. From a real-time operations perspective, whereas loss of individual bulk power generating stations is significant (potential for high impact on grid reliability), it is rare that loss of a single power station will cause wide-scale outages. The same is true for individual substations. However, loss of a single facility could cause a problem depending on the situation. The 2008 Florida blackout is an example where a single substation failure caused a blackout over a significant part of a state [15].

The impact model shown in Fig. 2 is assumed to be fairly typical of how control rooms are an integral and critical part of real-time grid operations. In this model, both the control room and the transmission grid itself are shown as having the potential for high (catastrophic) impact should an outage occur. Even though it may not be true in all cases, in this proposed model individual power plants and distribution infrastructure are assumed to have the potential for medium impact on grid reliability. Individual distributed generation (DG), distributed storage (DS), and frequency responsive reserve (FRR) resources are assumed to have the potential for low impact on wide area grid reliability. Individual distribution-focused systems such as the Advanced Metering Infrastructure (AMI), home area networks (HANs), and building management systems (BMSs) are also assumed to have low impact on grid reliability. (The authors concede that inadvertent or malicious activity resulting in changes to thousands or millions of AMI/HAN/BMS devices can have wider impact on regional grid operations, but discussion of such failure modes is outside the scope of this paper.)

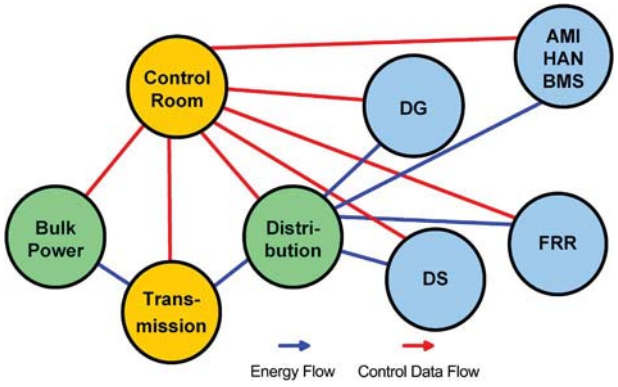

Fig. 2. ***Typical view of criticality (Control Room = High Impact).***

The new approach which our analysis yields is that, for real-time grid operations, a loss of reliable control over grid components, even if lasting several hours, should not result in a catastrophic outage in the reliability of the grid itself. This new view is reflected in Fig. 3.

The difference between these views (Figs. 2 and 3) is that in the latter view, a control room failure is not viewed as creating the potential for high/catastrophic impact on real-time grid operations.

This is not to suggest that the control room is unimportant. Due to the complexity of control room systems such as state estimators, we fully recognize that control room systems are vitally important to long-term grid operations. The difference in approach, however, is to note the distinction between doing a state estimator analysis, and issuing the command sequence to implement the recommendations of that state estimator analysis. Therein we see a critical design change being advocated.

Grid operators should continue to use their existing and emerging tools to determine what-if scenario responses, as is common today. What is less common, however, is that the results of the what-if analysis should be preloaded onto distributed sensors, actuators, and controllers outside the control room. That in and of itself will limit the impact that loss of reliable control from a control room or communications link can have on grid operations.

The ideal condition, of course, is for substation and field devices to do their own what-if analysis based on direct communications with a number of adjacent sensors. In the Aurora experiment [16] a generator was sent improper commands that resulted in its destruction. If the generator's own controls had the ability to directly sense local conditions and compare those conditions to what would happen if the commands being sent were executed, that attack would have been prevent from causing damage. While the attack may still have caused that generator to stop being a reliable asset in a microgrid, being able to do its own what-if analysis could have prevented the damage itself.

IV. DEFENSE IN DEPTH DISCUSSION

A defense-in-depth security model, as referenced above with application to the aviation industry, is critical to achieving a High Assurance Smart Grid. A robust cybersecurity architecture will involve the application of layered security controls to protect critical elements in electrical utility control networks. Fig. 4 shows a representative high level defense-in-depth model for an electric utility control center. This same model was shared with the NERC Smart Grid Task Force as the group's report was drafted [17].

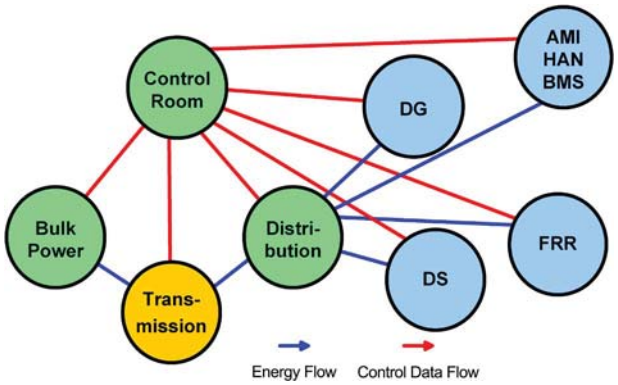

Fig. 3. ***Proposed view of criticality (Control Room = Medium Impact).***

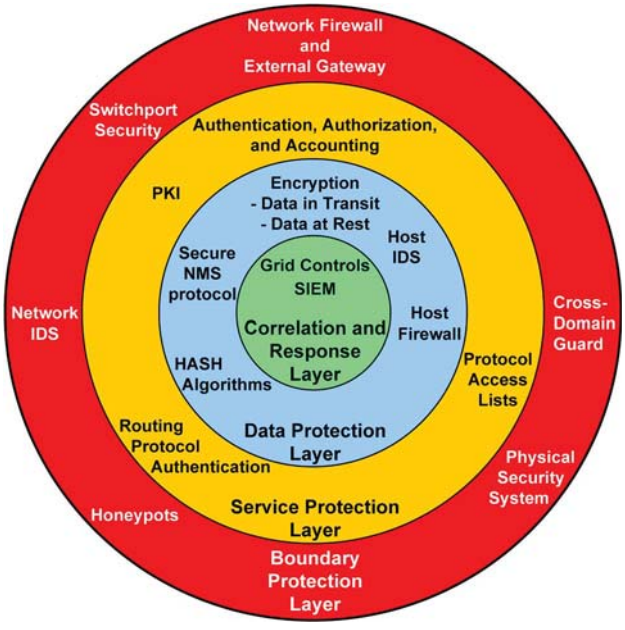

Fig. 4. ***Utility control center defense in depth model.***

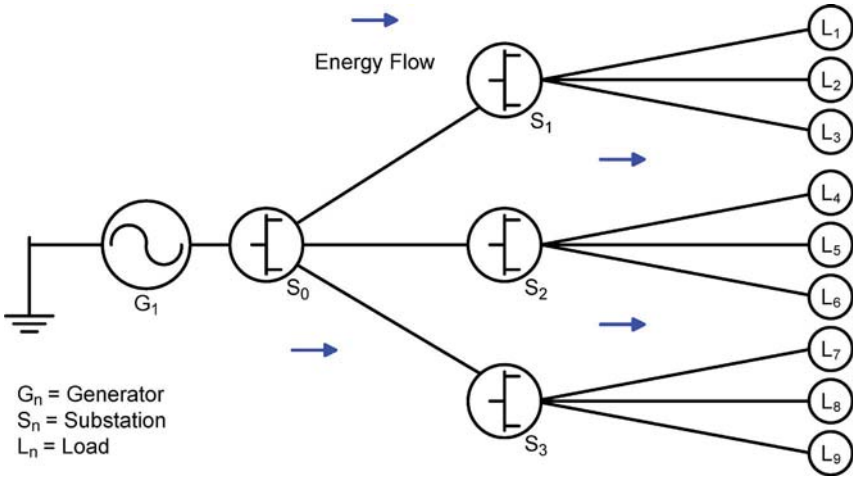

Fig. 5. ***Simple tree graph of energy flow.***

This model categorizes cybersecurity controls within the following set of layers:

Boundary protection layer. Contains controls for the cyber- and physical perimeter of the control center. A network demilitarized zone (DMZ) is considered part of the cyberperimeter. Example controls include firewalls; physical security devices such as surveillance cameras and intrusion detection/prevention sensors; access security, including wireless access point security and switchport security; and honey pots (security resources whose value lies in being probed, attacked, or compromised). Since the control center is a manned facility within a building, it is assumed the majority of physical security concerns for the control center will be addressed by general building physical security controls.

Service protection layer. Contains controls for access to services and applications for users inside of the HASG cyber/physical perimeter. Example controls at this layer include PKI, key management, role-based access control (e.g., authentication, authorization, and accounting), and protocol access lists.

Data protection layer. Contains controls to protect data within the HASG perimeter. Example controls include file integrity checking, host-based intrusion detection systems (HIDS), secure network management protocols such as SNMPv3, encryption of data in transit and data at rest, host-based intrusion detection and security, authentication of routers for a given routing protocol, and host hardening procedures from the Department of Homeland Security (DHS) and/or Department of Defense (DoD).

Correlation/response layer. Contains controls to perform correlation of and response to security incidents. Example controls include a security information and event management system (e.g., ArcSight), event correlation, log scanning, and incident response by a human security analyst.

Certain cybertechnologies may cut across multiple layers in the defense-in-depth model. One such technology utilizes distributed cyberagents residing on multiple control host computers throughout the environment. These agents may perform a variety of local functions, such as intrusion detection, log scanning, and event correlation. Such agents are receiving interest in DHS and DoD mission networks.

V. GRID CONTROL ARCHITECTURE

The original power distribution grid itself implemented a tree or radial hub and spoke topology. As transmission systems came on line, these too initially implemented the same topology, as illustrated in Figs. 5 and 6. An analysis of the two graphs reveals that the energy flows are equivalent. Thus whether the term "tree" or the term "radial" is used, in this context the terms are equivalent. The common attribute is that both the tree and the radial view are hierarchical rather than distributed in nature.

The modern grid includes, within each interconnect, hundreds of large-scale generators, hundreds of thousands of large industrial customers, and millions of commercial and residential customers. As the years have progressed, most transmission and some distribution operators have increased system reliability by the introduction of numerous interconnects or interties, Fig. 7, between various intermediate nodes.

These interties [18] provide paths between generators and loads. Some interties provide increased capacity, and some are purely for reliability purposes—if a primary path were to fail, there is an alternate path already installed. This redundancy can increase reliability by reducing both outage frequency and outage duration.

These simplified diagrams show how energy flow has been managed in various parts of the transmission and

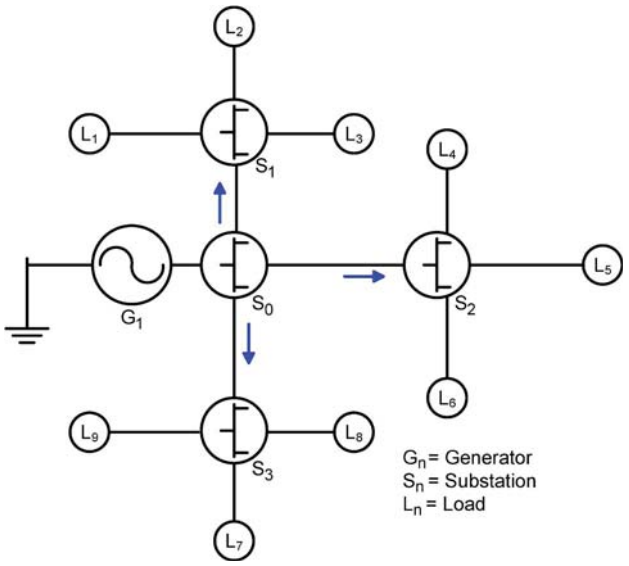

Fig. 6. ***Simple radial graph of energy flow.***

distribution grid for many years. It is interesting to note, however, that whereas *energy flow* is now more interconnected and less hierarchical, the energy *control system architecture* is still largely hierarchical.

Grid devices have three basic modes: manual control, automatic control, and remote control. (There is also a data load or maintenance mode, which is outside the scope of this paper.) Manually actuated devices need no further description. Automatic devices, as defined here, are primarily self-preservation type devices. These and similar devices combine a local sensor, controller, and an actuator, often in a single unit. Automatic circuit breakers are a classic example of an entirely automatic device. Automatic reclosers are another such device. While more sophisticated than circuit breakers, automatic reclosers historically were electromechanical devices that made a fixed number of attempts to reclose an electrical circuit in order to reenergize the affected line. Manual devices, as defined here, are excluded from the subject of interest for this paper. Programmable electronic sensors and actuators are most of interest for this discussion.

The network shown in Fig. 8 is based on the original electrical grid (see Fig. 2). It reflects the control data flow in a primarily hierarchical manner, where field device control is subordinate to the relevant substation, and where substations are subordinate to control room data flows.

In this model (see Fig. 8), which is typical of most control room environments these authors are familiar with, there is little if any peer communication or autonomous coordination between field devices and between substations. Each field device and substation has essentially automatic modes of operation, where decisions are fairly binary in nature and can be made based entirely on the state of local sensors. While substations and field devices in this scheme can and do make locally preprogrammed actions, decisions requiring higher complexity or broader grid considerations are typically beyond the capacity of these devices.

For decisions beyond self-preservation (such as circuit breakers), or actions by devices such as automatic reclosers [19]–[21], substations to some extent and field devices almost exclusively rely on receiving commands from

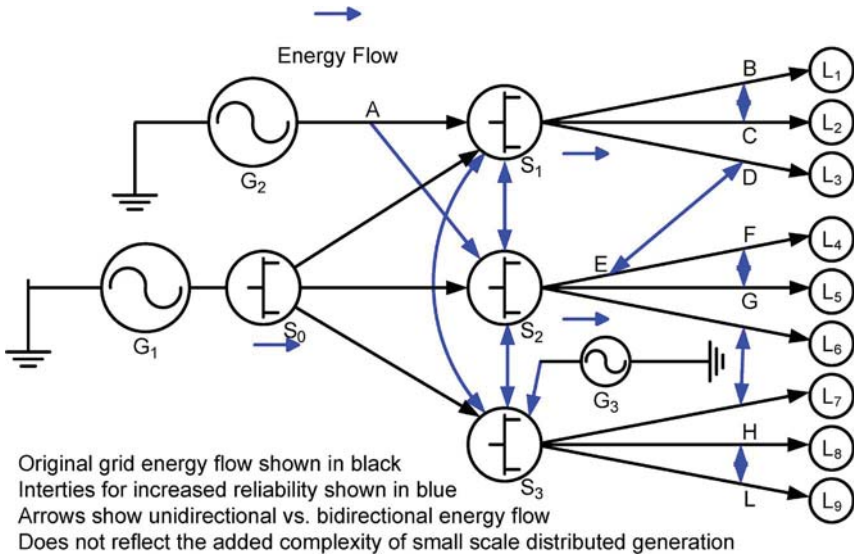

Fig. 7. ***Interconnected energy distribution.***

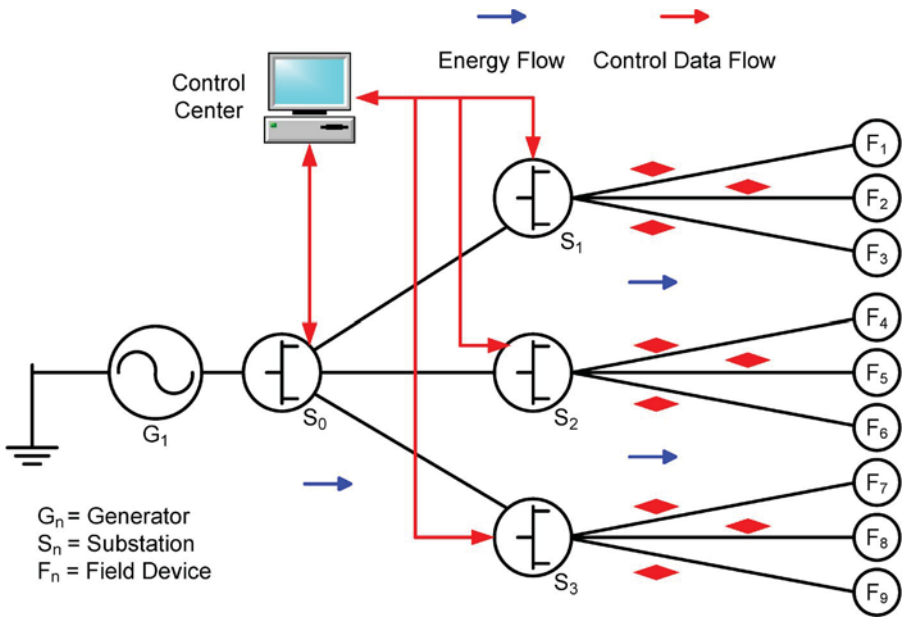

Fig. 8. ***Hierarchical grid control data flow.***

higher echelon control rooms, as is shown in Fig. 9; thus, whereas electrical power flow within the grid is far more interconnected than in past years, the control system data flow is still predominately hierarchical.

The result of this scheme is that most energy control today is still based on a hierarchical model of the original grid built 100 years ago. Herein lies a significant challenge and opportunity as we build a "Smart Grid" for the future.

Fig. 10 shows the combination of grid interties already widely implemented, with increased coordination between intelligent electronic devices (IEDs) in a manner not entirely dependent on control room input.

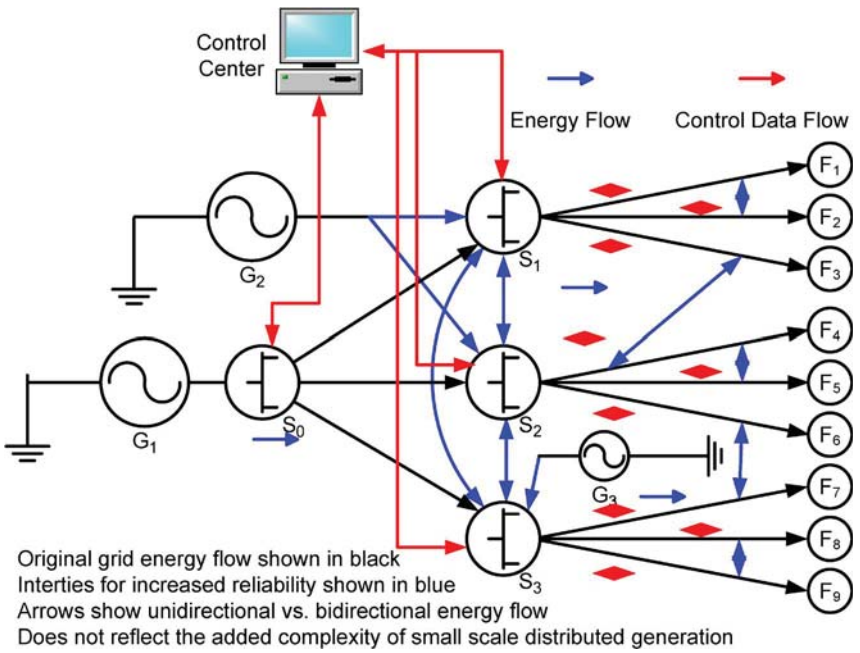

Fig. 9. ***Interconnected grid with hierarchical control.***

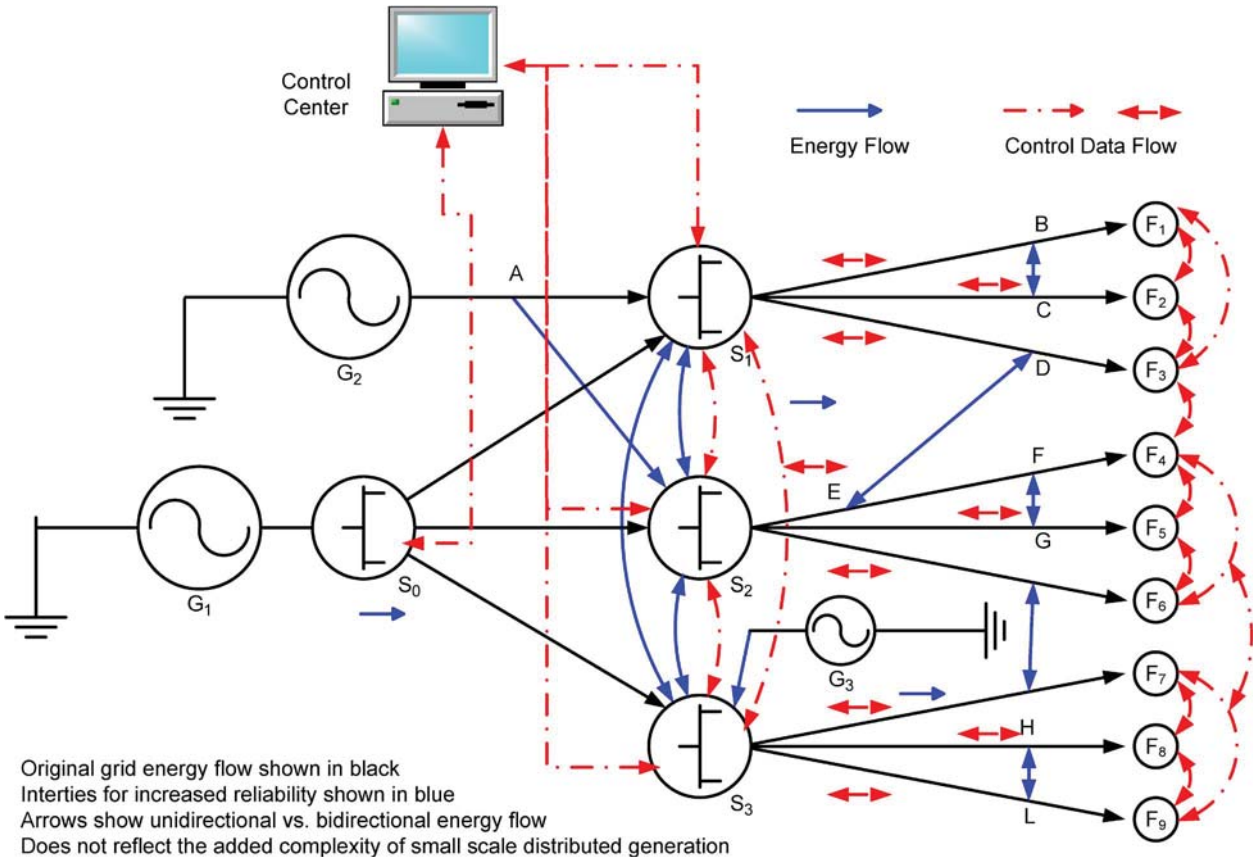

Fig. 10. ***Interconnected grid and grid control.***

In this new control system architectural model, field devices have some ability to sense peer devices beyond their traditional world view. Substations have the ability to collaborate across wider areas, again, without the requirement for this communication and control signaling to be done exclusively through control rooms.

It is noteworthy that this proposed architecture makes no attempt to eliminate lines of communications and control data flow between field devices, substations, and control rooms. Instead, the focus is on enhancing the distributed control signaling architecture such that some level of device collaboration can be done *even when there are losses of control capability from the still dominant hierarchical control system architecture*. This is a key feature required for a self-healing grid.

The loss of reliable control capability may emanate from a wide variety of failure modes. Among them are the following:

1) communications link failure;
2) sensor, controller, and/or actuator failure;
3) unplanned control center system failure;
4) nonexistent, late, or improper commands by untrained and/or distracted control room personnel.

It is also noted that rather than characterize malicious activity as a separate category, failure modes 1–3 above could be caused either by inadvertent/unplanned hardware/software failures or by malicious activity initiated by disgruntled employees or external attackers.

That concept is central to the recommended approach: *focusing cybersecurity efforts just on preventing external attack is not sufficient*.

For this paper, "loss of reliable control" is assumed to be caused by any of these failure modes. Whereas some failure modes result in *complete* loss of control, other failure modes result in loss of *reliable* control. We will make no distinction between these nuanced definitions and will use the term "loss of reliable control" throughout.

Key to this architectural model is that all such failures are to be addressed without extensive and sometimes distracting discussions focused on the likelihood of failure caused by an external attacker. In reality, the goal of most external attackers is to gain insider access. Thus if the control system architecture can limit damage caused by untrained and/or distracted utility personnel, or by unplanned control link or control system outages, it will

inherently be more resilient—and in the end will be more reliable—against attack by malicious actors.

The U.S. Department of Energy has long promoted the goal of an autonomous, self-healing grid [22], [23]. While it is unlikely there will ever be a truly autonomous and self-healing grid that manages itself independent of any human-in-the-loop (HITL) control system, striving toward this goal has significant benefits from a cybersecurity perspective.

Analysis of the 2003 Northeast blackout, the 2008 Florida blackout, and others shows that many widespread outages occur without any evidence of malicious activity being involved. Instead, these outages occurred because of a combination of anticipated factors. For the Northeast 2003 blackout, there were four primary causes [24]:

1) inadequate system understanding;
2) inadequate tree trimming resulted in multiple 345-kV and 138-kV transmission lines failing when they sagged into vegetation;
3) control system and communications failures at the operating utility did not give control room operators sufficient visibility to the outages within their territory;
4) a concurrent control system failure and inadequate data feeds at the Reliability Coordinator did not allow the operators sufficient visibility into the transmission failures within the transmission operator's territory.

Had the operators at the local utility and the regional balancing authority retained visibility into the current state of the transmission grid, it has been stated that the blackout likely would not have occurred. This is because normal control room system functionality was still available and would have enabled grid operators to determine the appropriate next steps to route power around the failed transmission line.

It is entirely appropriate for there to be significant focus on control system reliability that would decrease the likelihood of similar occurrences in the future. If, however, that is all that is done, then grid sensors and actuators will still be entirely reliant on receiving the next set of instructions from a hierarchical control room. In addition to increasing the reliability of the control systems themselves, distributed grid sensors and actuators must be given either more autonomous capability or, at a minimum, be preloaded with next-step instructions for actions to be taken in case of a variety of failure modes. For this to be effective, it is imperative that distributed sensors and actuators gain a wider world view than just sensing their immediate surroundings and sending data up/down a hierarchical control flow.

The Report of the 2003 Blackout lists the first violation as "Violation 1: Following the outage of the Chamberlin-Harding 345-kV line, [the transmission line operator] did not take the necessary actions to return the system to a safe operating state within 30 min [25]." There are, of course, multiple ways to avoid this situation in the future. The most common approach is to increase the reliability of the sensor and actuator network, increase the reliability of the control room systems themselves, and provide enhanced training for control room operators. This, however, misses a key point: control room systems and control data links are likely to fail again. In the world of aviation we would consider the control room as a whole as a single-point failure: disable the control room (physically or electronically) and you risk disabling the system. Which failure mode causes the loss of reliable control is relatively immaterial. Most bulk electrical system operators have redundant facilities to take control should the primary control centers be unavailable, but that is still insufficient for addressing modern vulnerabilities. Whether due to inadvertent failure, error, oversight, or malicious action, loss of reliable control should be *planned for* by building corrective mechanisms into distributed actuators in the grid. Thus we see that it is the very hierarchical nature of the control system that is the design flaw to be changed.

From a practical perspective, it would likely be infeasible to have all grid devices preloaded with corrective actions for all possible electric or control system failures. The IEEE 39-bus system shown in [26, Fig. 13.35], demonstrates this quite well. In that figure, there are 10 generators, 39 buses, and 51 links. Even if the only failure mode were complete failure of any link or node (an open circuit), there would be 100 failure modes. In reality, there are many times that number, because there are more failure modes than open circuits (current, frequency, and voltage variations for example), and there is the high likelihood during congested periods of having more than one simultaneous failure. Of course, not all failure modes are equal. Many grid devices are sufficiently isolated from each other, and there is no requirement for all devices to be able to compensate for all failure modes. This drives the level of intelligence that devices will need in order to ensure they can operate through failure.

VI. HASG TRUST MODEL: ASSUME COMPROMISE

As noted earlier, establishing an all-encompassing sphere of trust for Smart Grid controls is neither possible nor desirable. This is true whether considered on a regional/national basis or an individual Utility basis. In addition to distributing communications and decision-making capability, control room, substation, and field devices must have the ability to sense when to trust—and when not to trust—received sensor and command inputs. This is a particularly challenging area but one well worth considering.

Compromise must be assumed in grid control systems. In addition to the assumption of outright failure (missing data), this section is more explicitly about incorrect sensor and command information, whether inadvertent or

malicious in nature. Much research and development has been done in the areas of intrusion prevention systems (IPSs) and intrusion detection systems (IDSs). In part this is because components to solve problems in this area are definable, and commercialization of such system components is fairly straight forward. We are not suggesting that the overall problem is simple but that IPS and IDS component systems are well definable and therefore a variety of vendors have developed solutions in this area.

Fault-tolerant systems have long been researched and engineered. System redundancies and failover systems are examples. Intrusion-tolerant systems (ITSs) represent a related but newer field of research. There are a number of publications addressing this, papers [27] and [28] among them. The concept of an ITS approach is that while implementation of IPS and IDS systems is important, quite often these systems prove ineffective at preventing system intrusions. Security systems occasionally fail to perform their intended functions for a variety of reasons.

Perhaps more importantly, a focus on just IPS and IDS solutions fails to account for failure modes caused by distracted or untrained insiders. It also fails to account for insiders with malicious intent. An ITS, however, can account for these failure modes. As a general approach, addressing the insider threat (whether error- or malice-driven) has significant merit. It accommodates failures of IPS and IDS, and it focuses on what an outside attacker generally attempts anyway—to gain insider privileges. An ITS focus also addresses the fact that unpredictable people are already within whatever sphere of trust could be built.

For the electrical grid, a non-ITS approach is shown in Fig. 11. Most of interest for this discussion is that the substation or field device has implicit trust in the commands received from the control room. The sensors transmit information to the control room, the control room systems (or the operator) determine whether or not to close the switch, and the switch closes when instructed to do so. In this case, the power on the two sides of the switch is out of phase. Still, the actuator works in a state of blind trust on the assumption that the command received from the supervisory control and data acquisition (SCADA) represents a reasonable command.

The "Aurora Generator Test" cyberattack simulation conducted by Idaho National Lab demonstrated these conditions quite effectively [29]. There was nothing particularly magical about the attack. The attackers just issued commands for the generator to connect to the grid out of phase. Since the controller on the generator had no ability to synthesize sensor data that would have told it the power was out of phase, it merely did what it was told. This resulted in its destruction. While there is good work coming from that test in the area of increasing the security capabilities of the control infrastructure, there is little being done to increase the ability of field devices to sense for themselves whether command inputs received are reasonable to execute.

The better model for the electrical grid control systems is for the substation, field devices, and power plants to have the ability to independently validate the reasonableness of commands received (assuming they are untrusted)—and to do so in a way well beyond self-preservation tests. Fig. 12 illustrates this scheme.

In this view, the remote sensors still communicate with the control room, and the control room still sends commands to the remote actuators. The distinction in this view is that there is sufficient distributed intelligence for the remote devices to synthesize information from distributed sensors and from the control room in order to determine whether or not to actuate.

This method compensates for malicious commands, for erroneous instructions sent by the untrained or distracted control room operator, and for nonexistent commands as may happen when there is a failure of the control systems themselves. It is this latter part that has the most significance for moving toward the goal of an autonomous, self-healing grid [23].

An architecture that gives substation and field devices the ability to validate not only the integrity but also the reasonableness of commands received also gives an architecture where devices can have a wider world view than just self-preservation activities. This is also the control system architecture that will be needed in order to create more autonomy and self-healing capabilities for the grid, not just for individual grid devices. It is this control model (see Fig. 12) which enables the substation and field devices to do their own what-if analysis. Being able to determine when to trust or not trust received commands and to determine the impact of received commands before

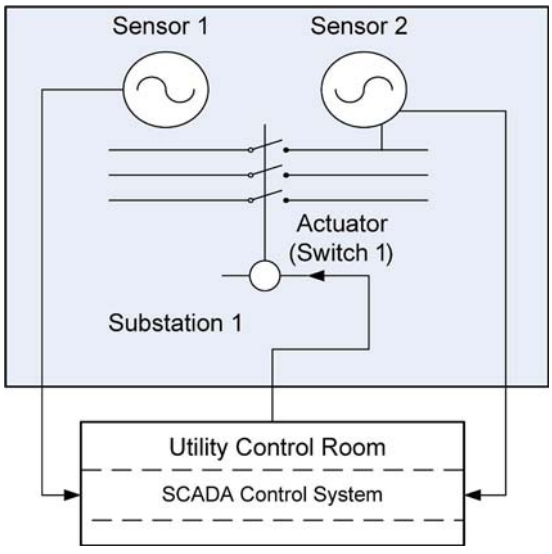

Fig. 11. ***Traditional hierarchical view of grid control.***

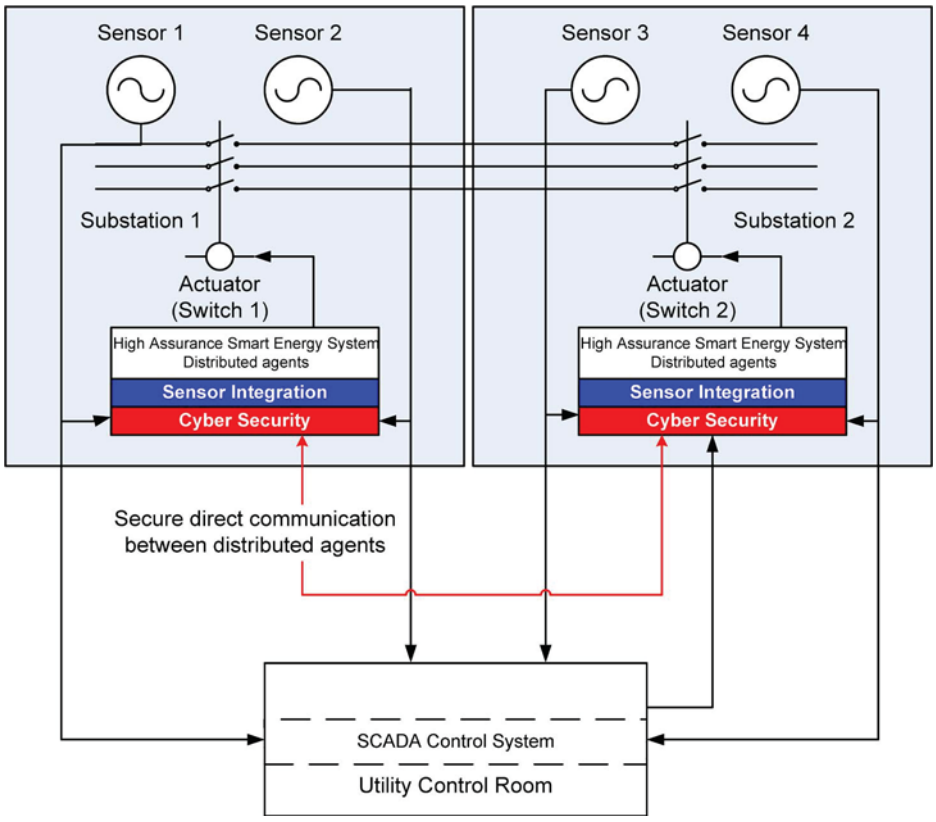

Fig. 12. ***High assurance smart grid control.***

taking action will provide significant benefit to the reliability of the grid itself.

VII. AUTORESPONSIVE LOADS AS A CYBER SECURITY COUNTERMEASURE

Earlier, we discussed how aircraft systems reliability is enhanced by reducing software code to the absolute minimum required to accomplish the intended function. In grid systems this design philosophy can be used to accomplish better load management while avoiding cyberattacks. The authors recognize that inherent in the process of building a smarter grid we will of necessity be increasing the complexity of grid controls. These may seem to be conflicted design principles, but increasing deployment of smart devices does not imply that we must abandon the principle of Least Functionality [10], [30] design. Section VI, above, discusses the Trust Model and increasing the ability of IEDs to determine the impact of received commands. This section, in contrast, explores the impact of true autonomy in the reliability of the grid. While this section uses examples related to consumer-owned appliances within a HAN, the same principles are applicable to many BMSs and industrial loads.

In part to enable greater load control for utilities, many current Smart Meter projects are attempting nothing less than to build a series of control systems with tens of millions of nodes (water heaters, clothes dryers, air conditioner compressors, etc.) in the distribution grid of some of the largest utilities. When viewed on a national scale, this increases to potentially many hundreds of millions of managed devices on electrical networks together with their corresponding nodes on control networks. It is well recognized that in such a system, each node represents a new point of system vulnerability that must be analyzed to understand and mitigate the impact of an attack or other compromise from that entry point. This leads to legitimate concerns about the ability to compromise those systems to create grid instability or to glean personal information as simple as indications of when consumers are or are not at home.

A risk/benefit analysis of such an extended control system, or even of just a system of loosely coupled control systems, may yield benefits from a cybersecurity perspective. There are, for example, several benefits to a system that has two-way communications and control all the way from the Utility to individual consumer-owned appliances in a home, among them is the availability of more refined consumer information that will enable power planning on a far more granular basis than is possible today. Additionally, the level of load control available to utilities will be much greater than with just the traditional paging system-based

load controls available at the consumer level—without the requirement to attach utility-provided hardware to each appliance being controlled.

There are also risks inherent in such an architecture, among them the cybersecurity concerns associated with having a relatively insecure communications path from the consumer into the Utility control room. After all, with consumer appliances being mass produced, it is unlikely that a rigorous level of security will be possible between the meter and the home appliances—and building meters that are also network security appliances will likely increase their cost and potentially decrease their service life. Lastly, there is the inherent possibility of consumers sending false load control response signals to a Utility in order to realize cost benefits while not actually reducing the load.

We will leave a more detailed discussion of the benefits and risks to other authors, because the point to be observed here is that rather than trying to build secure control systems with, collectively, hundreds of millions of nodes on a national scale, we should make load devices truly "smart" by increasing the ability of devices to autonomously sense and respond to grid conditions. We should make electrical loads autoresponsive rather than static.

Elasticity in electrical loads is often discussed in terms of pricing functions, such as in [31]. In conjunction with that view, achieving load elasticity is often seen in terms related to explicit load control to minimize costs during peak times. In this paper we use the term "autoresponsive or AR load" to describe a more fundamental approach related directly to the grid electrical conditions themselves rather than to the market implications of grid conditions.

Building secure two-way communications between a distribution utility and its home meters is a nontrivial but necessary challenge. It should be noted, however, that two-way communications between the utility and the meter do not require two-way communications between the meter and consumer-owned home appliances. Considering just the cybersecurity implications, having only one-way communications from a meter to consumer-owned devices reduces the attack surface of the meter itself. If the meter does not listen to communications from consumer-owned devices, no attack from that direction is possible. This approach may also reduce the complexity, cost, and potential failure modes of consumer-owned devices themselves.

Where desired, dynamic pricing signals can still be sent one way from the meter to consumer-owned appliances. Strictly from a power management perspective, however, the knowledge that it was a water heater vs. a clothes dryer that reduced load would seem to be of little if any benefit to a utility. In any case, receiving a pricing signal acknowledgment from an appliance does not mean the appliance actually reduced load. Confirmation of whether consumer-owned devices responded to a price signal can easily be determined by measuring the power flowing through the meter which, after all, is the meter's primary function.

As an alternative approach to explicit utility control over consumer appliances, or at least as a complimentary approach, appliances can be given the ability to directly sense and respond to grid instability. A 2007 report by Pacific Northwest National Lab [32] described a test implementation of this concept. In that study, devices were programmed to respond to under-frequency conditions by automatically reducing load when the electrical frequency was below 59.95 Hz. Expanding that model, similar technology can be used to have loads automatically serve as distributed load banks by having devices such as water heaters *take on load* for short periods of time whenever the line frequency *exceeds* a limit, such as 60.05 Hz. Similarly, devices can be given the ability to sense when line voltage sags or surges from the average incident line voltage at the specific location. This logic would be needed for voltage sensing, which varies based on where a device is in the distribution grid, whereas frequency fluctuations are felt system-wide, even across an entire interconnect region.

When considering AR load shedding or load increases based on either voltage or frequency variations, care must be given so that grid instability is not created from having a large number of devices connect to or isolate from the grid in unison. To alleviate this condition, we might consider a data networking protocol that provides a parallel for a method of creating AR loads: The well-documented Ethernet protocol uses a system of carrier sense multiple access/collision detection (CSMA/CD). The CSMA/CD networking protocol is described in detail in IEEE 803.3 [33]. Stated in a very simplified manner, CSMA/CD works in the following way:

1) Carrier sense (CS) means that before sending a packet, check to see if another packet is already transiting the data network. If there is already traffic on the data network, then wait before putting more packets onto the data network.The grid parallel is that elastic loads should monitor voltage and frequency (which is much simpler than implementing a two-way data communications capability) before deciding to increase the load on the electrical network.
2) Multiple access (MA) just means that several devices share the same data network.The grid parallel is that many loads share the same electrical network.
3) Collision detection (CD) in 802.3 was developed to address the likelihood that even when devices do the appropriate CS verification, data collisions (multiple packets on the data network at the same time) will still occur. In these cases, devices are programmed to stop transmitting, listen again for a quiet time on the network, and wait a

randomized amount of time before attempting to use the data network again.

The grid implication is that AR load devices should be able to sense—and respond to—grid duress without having to wait for instructions from a control system. They should also have a mechanism that uses a random function to manage how masses of devices collectively respond to grid conditions. Aside from the cost avoidance by simplifying control system architecture, AR loads would also be more responsive in real time. Hierarchical control implies a process of sense—transmit—synthesize—decide—transmit—action. AR loads would go directly from sense to action, without any of the cost, complexity, latency, or vulnerabilities of the hierarchical approach.

The random aspect of CD is a key feature for both data and electrical network devices. It exists to limit the risk of heavy traffic or load resulting in dramatic fluctuations in network demand. In both data and electrical networks that load oscillation can have a devastating impact on the stability of the network in question. In 802.3 networks the random retry delay is measured in milliseconds, microseconds, and nanoseconds [33]. For an electrical network the retry delay is likely to be a range of minutes to tens of minutes.

The cybersecurity implication of such a model for autonomous, AR loads is that, since there would be no control system built, no control system would be available for compromise (whether inadvertent or intentional). Thus the scenario of widespread grid instability caused by compromising large numbers of loads would not be available to an attacker. Indeed, it is today's lack of autoresponsiveness that creates the perceived requirement for explicit load control. From an energy management perspective, having loads that are able to self-regulate demand will substantially obviate the need for explicit control.

VIII. CONCLUSION

There is no single solution to Smart Grid Cybersecurity. It is only through the application of a combination of approaches that grid control systems can be sufficiently engineered for both the electric service reliability already expected and the cybersecurity implications emerging with new sensor and actuator technologies.

A High-Assurance Smart Grid architecture must:

1) Categorize cybersecurity requirements based on a three-tier determination of a subsystem's potential impact on the overall system;
2) Implement a robust defense-in-depth cybersecurity architecture;
3) Implement a distributed rather than hierarchical control system architecture, with a trust model based on the assumed compromise (untrusted condition) of control system components and subsystems, and using AR load control wherever possible to achieve demand-response without the vulnerabilities inherent in all command and control systems.

IX. AREAS FOR FURTHER RESEARCH

There is no expectation that the full complexity of transmission or distribution control room state estimators and other applications will be miniaturized and installed on single-board computers of substation and field devices. However, there is a significant amount of research and development work in the areas of autonomous robotics [34] and multi-agent coordination [35]–[40] which provide examples for how grid devices can work with limited individual capability and yet manage, together, more complex operations than any individual device could do on its own. In addition, further research in the area of intrusion-tolerant systems in the electrical or other control systems environments could have significant value.

Another area of exploration is in the evolution of grid controls and grid security, focusing on both the installed base as well as newly installed systems. While there are vendor solutions that use additional security hardware inserted into the communications links, there are methods of increasing the inherent security capabilities of many installed grid devices which should also be explored.

AR load control is yet another area for additional research. Particularly of interest would be modeling and simulation of such systems when implemented on a large scale. Intuitively the parallels to CSMA/CD mechanisms used in data networks seem applicable to electrical networks. The PNNL study [32] mentioned earlier provides an example of the effectiveness of this in a relatively small scale implementation. Utilization of this method for potentially millions of devices in a large metropolitan area should be studied and modeled as well.

Transformation of the grid control architecture is a final and perhaps most obvious area for study based on the recommendations of this paper. The opportunity provided by the technological advances in control system components enables a rethinking of many aspects of how the electrical grid is managed. Two decades ago there was a significant effort to reengineer business processes in order to achieve higher levels of efficiency and effectiveness within and between enterprises.

The key principle of many of these efforts was to recognize the opportunity to reconsider how the work was done, not just how to automate formerly manual processes. An important work from that time pointed out that over time, "We have institutionalized the ad hoc and enshrined the temporary [41]." Rather than viewing the increasing capability of advanced grid control sensors and actuators to provide merely higher fidelity sensor information to control room systems, or to provide remote control of increasing numbers of field and consumer owned devices, these increased capabilities should be viewed from the

Table 1 Acknowledgments

Name	Organization
Roger Anderson	Columbia University
Sandy Bacik	EnerNex Corporation
Mark Baenziger	Boeing Defense, Space and Security
Aaron Bennett	North American Electric Reliability Corporation
Jeff Dagle	Pacific Northwest National Lab
Frank Doherty	Consolidated Edison Co. of New York
Erfan Ibrahim	Electric Power Research Institute
Marija Ilic	Carnegie Mellon University
Chris Kotting	ckotting.com consulting
Arthur Kressner	Consolidated Edison Co. of New York
Annabelle Lee	Electric Power Research Institute
Claudio Lima	Sonoma Innovation
Michael Peters	Federal Energy Regulatory Commission
Thomas Peterson	Boeing Defense, Space and Security
Steve Weismuller	Boeing Defense, Space and Security
Joe Weiss	Applied Control Solutions, LLC

perspective of enabling far more distributed control, autonomous communications, security, and device collaboration than has been possible in the past. ■

Acknowledgment

While numerous citations appear in the following section, this paper predominately represents the original research, analysis, and conclusions of the authors. As with many collaborative efforts, this work is also based on formal and informal discussions with a number of colleagues from throughout industry and government. The authors wish to express their appreciation to the individuals in Table 1 for contributing to our understanding of the many complexities of and approaches to Smart Grid Cyber Security.

REFERENCES

[1] J. Weiss, *Protecting Industrial Control Systems From Electronic Threats*. Highland Park, NJ: Momentum Press, 2010, pp. 116–118, 121, 128–135, 140, 142–143.

[2] *Federal Aviation Administration Advisory Circular AC-25.1309-1A*, Jun. 21, 1988.

[3] *Software Considerations in Airborne Systems and Equipment Certification*, DO-178B, Radio Technical Commission for Aeronautics (RTCA), Issued 12-1-92, Errata Issued 3-26-99.

[4] I. Yen, R. Paul, and K. Mori, "Toward integrated methods for high-assurance systems," *Computer*, vol. 31, no. 4, pp. 32–34, Apr. 1998.

[5] *Information Technology—Security Techniques—Evaluation Criteria for IT Security—Part 3: Security Assurance Components*, Int. Std. ISO/IEC 15408-3, 2008.

[6] *Information Technology—Security Techniques—Evaluation Criteria for IT Security—Part 1: Introduction and General Model*, INCITS/ISO/IEC 15408-1:1999 (R 2005), American National Standards Institute, 1999.

[7] *Proc. 12th IEEE Int. High Assurance Syst. Eng. Symp.*, San Jose, CA, 2010. [Online]. Available: http://web.mst.edu/~hase/hase2010/

[8] D. Desovski, Y. Liu, and B. Cukic, "Linear randomized voting algorithm for fault tolerant sensor fusion and the corresponding reliability model," in *Proc. Ninth IEEE Int. High Assurance Syst. Eng. Symp.*, Heidelbery, Germany, 2005, pp. 153–162.

[9] *Industry Advisory, Protection System Single Point of Failure*, North American Electric Reliability Corporation (NERC), A-2009-03-30-01, 2009.

[10] "Standard practice for system safety," in *System Safety Handbook*, (Appendix H), 2000, p. 14, Federal Aviation Administration. [Online]. Available: http://www.faa.gov/library/manuals/aviation/risk_management/ss_handbook/

[11] *Manual on the Aeronautical Telecommunication Network (ATN) Using Internet Protocol Suite (IPS) Standards and Protocols (Doc 9896)*, 1st ed., International Civil Aviation Organization, 2010.

[12] *Spec 42: Aviation Industry Standards for Digital Information Security, Air Transport Association (Revision 2010.1)*, Air Transport Association of America, 2010.

[13] *NIST Smart Grid Interoperability Panel.* [Online] http://www.nist.gov/smartgrid/

[14] *Categorizing Cyber Systems: An Approach Based on BES Reliability Functions*, Cyber Security Order 706, Cyber Security Standards Drafting Team for Project 2008-06, North American Electric Reliability Corporation, 2009.

[15] *2009 Report on Enforcement, Office of Enforcement*, Federal Energy Regulatory Commission, Washington, DC, Docket No. AD07-13-002, 2009

[16] *Sources: Staged Cyber Attack Reveals Vulnerability in Power Grid*, CNN.com, 2007. [Online]. Available: http://www.cnn.com/2007/US/09/26/power.at.risk/

[17] *Reliability Considerations From Integration of Smart Grid*, North American Electric Reliability Corporation, Princeton, NJ, 2010, Smart Grid Task Force Report.

[18] M. H. Brown and R. P. Sedano, *Electricity Transmission: A Primer*. Washington, DC: National Council on Electricity Policy, Jun. 2004.

[19] *Reclosers and Controls*, Cooper Power Systems. [Online]. Available: http://www.cooperpower.com/products/Distribution/Reclosers/

[20] *Application Note: The Effect of Loop Reconfiguration and Single Phase Tripping on Distribution System Reliability*, ABB Inc. [Online]. Available: http://www05.abb.com/global/scot/scot235.nsf/veritydisplay/ce0cc4f93ec4e17f85256c41006a527f/$File/Distribution%20System%20Reliability.pdf

[21] *Siemens Vacuum Recloser 3AD*, Siemens AG, HG 11.42, 2008. [Online]. Available: http://www.energy.siemens.com/hq/pool/hq/power-distribution/medium-voltage-outdoor-devices/vacuum-recloser-3ad/HG-11-42-IUS-en.pdf

[22] B. Renz, "Anticipates and responds to disturbances (Self Heals)," in *Research on the Characteristics of a Smart Grid by the NETL Modern Grid Strategy Team*, U.S. Dept. Energy National Energy Technol. Lab, 2008.

[23] *A Vision for the Smart Grid*, U.S. Dept. Energy, Office of Electricity Delivery and Energy Reliability, National Energy Technology Laboratory, 2009.

[24] *Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations*, U.S.-Canada Power System Outage Task Force, 2004, p. 19.

[25] *Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations*, U.S.-Canada Power System Outage Task Force, 2004, p. 22.

[26] M. Ilic and J. Zaborszky, *Dynamics and Control of Large Electric Power Systems*. Hoboken, NJ: Wiley, 2000, p. 756.

[27] K. Meng, C. Lin, Y. Z. Wang, and Y. Yang, "Modeling and evaluation of intrusion tolerant systems based on dynamic diversity backups," in *Proc. ISIP*, Huangshan, P. R. China, 2009, pp. 101–104.

[28] F. Gong, K. Goseva-Popstojanova, F. Wang, R. Wang, K. Vaidyanathan, K. Trivedi *et al.*, "Characterizing intrusion tolerant systems using a state transition model," in *Proc. DISCEX 2001*, vol. 2, p. 1211. [Online]. Available: http://people.ee.duke.edu/~kst/security/DISCEX-II.pdf

[29] Energy Assurance Daily, Sep. 27, 2007, U.S. Dept. of Energy, Office of Electricity Delivery and Energy Reliability, Infrastructure Security and Energy Restoration Division. [Online]. Available: http://www.oe.netl.doe.gov/docs/eads/ead092707.pdf

[30] *Payment Card Industry (PCI) Data Security Standard*, Security Audit Procedures, Version 1.1 (Section 2.2.4), PCI Security Standard Council, 2006. [Online]. Available: https://www.pcisecuritystandards.org/pdfs/pci_audit_procedures_v1-1.pdf

[31] M. Ilic and J. Zaborszky, *Dynamics and Control of Large Electric Power Systems*. Hoboken, NJ: Wiley, 2000, p. 662.

[32] D. J. Hammerstrom, J. Brous, T. A. Carlton, D. P. Chassin, C. Eustis, G. R. Horst *et al.*, "Pacific Northwest GridWise Testbed Demonstration Projects: Part II. Grid Friendly Appliance Project," Richland, WA, Pacific Northwest National Lab Rep. PNNL-17079, 2007.

[33] *IEEE Standard for Information Technology—Telecommunications and Information Exchange Between Systems—Local and Metropolitan Area Networks—Specific Requirements, Part 3: Carrier Sense Multiple Access With Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications, Amendment 4: Media Access Control Parameters, Physical Layers and Management Parameters for 40 Gb/s and 100 Gb/s Operation*, IEEE Std. 802.3ba-2010 (Amendment to IEEE Std. 802.3-2008), 2010. [Online]. Available: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5501740&isnumber=5501739

[34] K. Konolige, C. Ortiz, R. Vincent, A. Agno, B. Limketkai, M. Lewis *et al.*, *Centibots: Large Scale Robot Teams*, Artificial Intelligence Center, SRI International, Menlo Park, CA, 2003.

[35] A. Agogino and K. Tumer, "Handling communication restrictions and team formation in congestion games," *J. Autonom. Agents Multi Agent Syst.*, vol. 13, no. 1, pp. 97–115, 2006.

[36] *Robotics and Autonomous Systems Research*, School of Mechanical, Industrial, and Manufacturing Eng. College Eng. Oregon State Univ. [Online]. Available: http://mime.oregonstate.edu/research/MIME_RAS_Robotics.html

[37] Boeing Trusted Software Center, Univ. Illinois at Urbana-Champaign. [Online]. Available: http://www.iti.illinois.edu/content/boeing-trusted-software-center

[38] P. Hines, A. Feliachi, K. Schoder, S. Hamilton, R. Yinger, and C. Vartaian, "Integrated, agent-based, real-time control systems for transmission and distribution networks," in *Proc. Grid-Interop Forum*, 2007.

[39] C. Holmes-Parker, *A Multiagent Approach to Managing Energy Production Facilities via Q-Learning*, class paper, Dept. Mech. Eng., Oregon State Univ., 2010.

[40] K. Turner and A. Agogino, "Distributed agent based air traffic flow management," in *Proc. 2007 AAMAS Int. Conf.*, Honolulu, HI.

[41] M. Hammer, "Reengineering work: Don't automate, obliterate," *Harvard Business Rev.*, vol. 68, no. 4, pp. 104–112, Jul./Aug. 1990.

ABOUT THE AUTHORS

Tom M. Overman (Member, IEEE) received the Bachelor of Arts degree in applied mathematics and physics from Warren Wilson College, Asheville, NC, in 1984 and a Master of Science degree in engineering management and leadership from Santa Clara University, Santa Clara, CA, in 1999.

He is the Chief Architect, Boeing Energy Cyber Security, Sunnyvale, CA. Prior to joining Boeing, he worked as a software product manager and program manager at firms such as ROLM and Applied Materials. He also has more than 30 years of service in the U.S. Navy Reserve. This includes both enlisted and commissioned service. Beginning in September 2001, he spent most of the next two and one half years on active duty, during this period serving as Defensive Information Operations staff officer for the military task force supporting the 2002 Olympics. Following that, he was assigned to support the Naval Security Group, the National Security Agency, and the U.S. Transportation Command. He is the author of numerous conference papers and has given presentations on Smart Grid Cyber Security to the U.S. Department of Energy, at industry conferences, at the Association of Computing Machines Cyber Security and Information Intelligence Workshop, and at the 2010 First IEEE International Conference on Smart Grid Communications (SmartGridComm). His main research focus is on finding ways to "design-out" vulnerabilities rather than just to compensate for them.

Mr. Overman is a Certified Information Systems Security Professional (CISSP), Information Systems Security Management Professional (ISSMP), and Project Management Professional (PMP). He is actively involved in the North American Electric Reliability Corporation (NERC) Smart Grid Task Force.

Ron W. Sackman (Member, IEEE) received the Bachelor of Science degree in electrical engineering and the Master of Science degree in electrical engineering/solid state electronics all from the University of California at Los Angeles (UCLA), in 1988 and 1990, respectively.

He is an Associate Technical Fellow for the Boeing Company, serving as Chief Network Architect for Boeing Applied Network Solutions in Sunnyvale, CA. Prior to joining Boeing in 2002, he was a Senior Network Consultant with International Network Services. He has coauthored several papers for IEEE conferences on the subject of smart grid cybersecurity. He has authored numerous internal Boeing papers on network-centric system design and cybersecurity. He is actively researching the applications of networking and cybersecurity technology to national critical infrastructure systems, including the power grid.

Mr. Sackman is actively involved in the IEEE Smart Grid Interoperability standards development (P2030) communications task force and is a regular participant in the Internet Engineering Task Force (IETF).

Terry L. Davis (Member, IEEE) received the Bachelor of Science degree in civil engineering from Oklahoma State University, Stillwater, in 1972 and the Master of Science degree in strategic planning for critical infrastructure from the University of Washington, Seattle, in 2007.

He is currently Chief Scientist for iJet Onboard, an aviation communications company in Seattle, WA, after having retired from The Boeing Company in October 2010, where he had been since 1984. At the Boeing Seattle location, he worked in aircraft simulation, network programming, and design, and served as Corporate Security Architect from 1997 to 2000. He left Boeing briefly, serving first as Operations Manager and then Vice President of Consulting for ViaLight, a "fiber-to-the-home" infrastructure company. He returned to Boeing in 2001 to work with the Connexion by Boeing Division, where he served as Chief Network Engineer and then in 2005, was named a Boeing Technical Fellow and became the division Chief Information Officer. In 2006, he moved to Boeing Commercial Airplanes, where he led work on Aircraft Communications, Network, and Security Architecture strategy and planning until 2010. In his earliest positions after graduating from college, he worked with the U.S. government for various agencies in the Departments of Defense, State, Energy, and the Interior.

Mr. Davis is a registered professional engineer in Oklahoma, Colorado, and Washington. He is a member of the American Society of Civil Engineers, is active in standards development in numerous international bodies, and has participated in various working groups for the Internet Engineering Task Force, Airlines Electronic Engineering Committee, and the International Civil Aviation Organization's Aeronautical Communications Panel. He has just completed a two-year appointment as a Council Member on the Internet Corporation for Assigned Names and Numbers' Generic Names Supporting Organization.

Brad S. Cohen received the Bachelor of Science degree in electrical engineering from the University of Massachusetts, Amherst, in 1981.

He joined The Boeing Company in 1980 and is currently the Director of Product Development and Chief Engineer of Boeing Energy, within Boeing Defense, Space and Security (BDS) in St. Louis, MO. During his time with Boeing, he has assumed increasing program management, design, and systems/system of systems engineering leadership responsibilities on multiple missile, aeronautical, and defense systems. In his 30 years with Boeing, he has held executive and nonexecutive leadership positions in both Engineering and Program Management. This includes assignments as Director of Systems of Systems Engineering and Integration on Future Combat Systems, Chief System Engineer of Air Traffic Management, Deputy Director of the Systems Integration Team and System Engineering Manager of the International Space Station.

Mr. Cohen is a Space Flight Awareness and Silver Snoopy award recipient and is a member of the Association of the United States Army. He is a father of three, and is actively involved in the Boy Scouts as an Assistant Scout Master.